

Statement of Work (SOW)
for the
Information Technology (IT) Security Program Assessment Review

1.0 **Purpose**

The <<YOUR AGENCY>> is seeking a Contractor to independently review <<YOUR AGENCY>>'s self-assessment of their IT Security Program.

2.0 **Background**

The *Government Information Security Reform Act, Title X, subtitle G of the 2001 Defense Authorization Act* mandates that each Agency perform an annual IT Security Program review based on the Chief Information Officer (CIO) Council's *Federal Information Technology Security Assessment Framework* published November 28, 2000. Guidance for agencies on implementing the *Government Information Security Reform Act* can be found in a *Memorandum for the Heads of Executive Departments and Agencies* published January 16, 2001 by the Office of Management and Budget. Guidance for agencies to self-assess their IT Security Programs is provided by the National Institute of Standards and Technology's (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* published September, 2001. <<YOUR AGENCY>> security staff will assess <<YOUR AGENCY>>'s IT Security Program by completing the questionnaire contained in the NIST Self-Assessment Guide. <<YOUR AGENCY>> will provide their completed questionnaire and related documentation to the Contractor for review.

3.0 **Objectives**

The Contractor shall independently review <<YOUR AGENCY>>'s self-assessment of their IT Security Program to determine if <<YOUR AGENCY>> has accurately determined the effectiveness level of <<YOUR AGENCY>>'s IT Security Program. In making this determination, the Contractor shall review <<YOUR AGENCY>>'s completed questionnaire consisting of approximately 47 pages and related documentation consisting of not more than 8,000 pages provided by <<YOUR AGENCY>>. The Contractor shall conduct interviews of <<YOUR AGENCY>> headquarters personnel as they determine necessary. The Contractor shall prepare a written draft and written final report.

4.0 **Suitability Clearances and Minimum Experience Requirements**

All Contractor personnel working on this contract shall have a minimum of a <<YOUR AGENCY STANDARD>> suitability clearance. At a minimum, Contractor personnel working on this contract shall have the required experience as follows:

Program Manager: Demonstrated, in-depth knowledge consistent with security principles and best practices as reflected in the CIO Council's *Federal Information Technology Security Assessment Framework*, *Government Information Security Reform Act*, *Computer Security Act*, Office of Management and Budget A-130 and NIST 800-18.

Ten years experience in consulting or conducting information systems security analyses or reviews.

Demonstrated experience in assessing large civilian or non-civilian government Security Programs.

Demonstrated experience in writing and presenting reports to Executive level personnel.

A college degree in Computer Science or Information Management
or

Currently a Certified Information Systems Security Professional (CISSP)

or

Documented experience in all 10 Common Body of Knowledge areas:

- Access Control Systems and Methodology,
- Telecommunications and Network Security,
- Security Management Practices,
- Application and Systems Development Security,
- Cryptography,
- Security Architecture and Models,
- Computer Operations Security,
- Business Continuity Planning and Disaster Recovery Planning,
- Law, Investigation, and Ethics, and
- Physical Security.

Support Staff: Three years experience which demonstrates knowledge in the area of Computer Information Systems Security.

5.0 **Scope**

The contractor shall provide all necessary qualified, experienced personnel to carry out the tasks in this agreement and meet the personnel requirements specified under **Suitability Clearances and Minimum Experience Requirements**. <<YOUR AGENCY>> shall supply the information as discussed under **Objectives**.

6.0 **Specific Performance Requirements**

Task One: Complete and Deliver Suitability Clearance and Building Access Forms

<<THIS SECTION SHOULD BE MODIFIED TO MEET YOUR AGENCY REQUIREMENTS>>

The Contractor shall, by the timeframe specified in the **Schedule of Deliverables**, complete and deliver to the <<YOUR AGENCY>> Project Officer a fingerprint form FD-258, Declaration for Federal Employment form OF-306 (available at <http://www.opm.gov/forms/html/of.htm>), Fair Credit Reporting Act Statement form, Application for Special Access to <<YOUR AGENCY>> Buildings and Special Agreement Form 86-C for each Contractor or subcontractor employee that will work on this contract. Fingerprints can be taken by <<YOUR AGENCY>> personnel at their central office located at <<YOUR AGENCY ADDRESS>> (forms are available at this location) or can be done at a local police station (original form FD-258 shall be used and will be provided by <<YOUR AGENCY>>). Each Contractor or subcontractor employee's completed forms shall be put into a separate envelope that is sealed and has the following information printed on or attached to the envelope:

Full Legal Name: _____

Social Security Number: _____

Date of Birth: _____

Place of Birth: _____

Position Title: _____

Previous Security Clearance: _____

Type of Clearance: _____

Date Obtained: _____

Obtained From: _____

Task Two: Post Award Meeting

The Contractor shall attend a post award meeting with <<YOUR AGENCY>> to discuss contract administration, deliverables, deliverable schedule and to clarify any issues, by the timeframe specified in the **Schedule of Deliverables**. This meeting will take place at <<YOUR AGENCY>> <<YOUR LOCATION>>.

Task Three: Research and Review of Documents

The Contractor shall, by the timeframe specified in the **Schedule of Tasks/Deliverables**, review <<YOUR AGENCY>>'s completed questionnaire and related documentation provided by <<YOUR AGENCY>>, review documents referred to under **Background**, conduct interviews (in person or via telephone) of <<YOUR AGENCY>> personnel as

Contractor determines necessary, and research and review any other documents as Contractor determines necessary. No travel expenses will be provided for interviews conducted under this task.

Task Four: Prepare and Deliver a Draft Report

The Contractor shall prepare and deliver, by the timeframe specified in the **Schedule of Tasks/Deliverables**, a draft report in typed and electronic form, as described under **Objectives** to the <<YOUR AGENCY>> Project Officer. For each question in <<YOUR AGENCY>>'s completed questionnaire, the draft report shall indicate the Contractor's agreement or disagreement with the <<YOUR AGENCY>> assessment. For each question in <<YOUR AGENCY>>'s completed questionnaire where the Contractor agrees with the <<YOUR AGENCY>> assessment, the draft report shall describe why the Contractor agrees with the <<YOUR AGENCY>> assessment and provide specific reasons and references that support the Contractor's position. For each question in <<YOUR AGENCY>>'s completed questionnaire where the Contractor disagrees with the <<YOUR AGENCY>> assessment, the draft report shall describe why the Contractor disagrees with the <<YOUR AGENCY>> assessment and provide specific reasons and references that support the Contractor's position. The draft report shall be delivered in typed and electronic form. The electronic form of the draft report can be delivered by e:mail or disk and shall be in Microsoft Word compatible format <<OR YOUR AGENCY STANDARD>>.

Task Five: Meet with <<YOUR AGENCY>> Personnel

The Contractor shall meet, by the timeframe specified in the **Schedule of Tasks/Deliverables**, with <<YOUR AGENCY>> personnel, as determined by the Project Officer, to discuss the draft report, their determinations, answer questions from <<YOUR AGENCY>> personnel and make a record such that discussion during the meeting is documented.

Task Six: Prepare and Deliver Meeting Minutes

The Contractor shall prepare and deliver, by the timeframe specified in the **Schedule of Tasks/Deliverables**, written minutes of the **Task Five** meeting. The minutes shall be delivered in typed and electronic form. The electronic form of the minutes can be delivered by e:mail or disk and shall be in Microsoft Word compatible format <<OR YOUR AGENCY STANDARD>>.

Task Seven: Prepare and Deliver a Final Report

The Contractor shall prepare and deliver, by the timeframe specified in the **Schedule of Tasks/Deliverables**, a final report in typed and electronic form, which reflects discussions held with <<YOUR AGENCY>> personnel under **Task Five** to the <<YOUR AGENCY>> Project Officer. For each question in <<YOUR AGENCY>>'s completed questionnaire, the final report shall indicate the Contractor's agreement or disagreement with the <<YOUR AGENCY>> assessment. For each question in <<YOUR AGENCY>>'s completed questionnaire where the Contractor agrees with the

<<YOUR AGENCY>> assessment, the final report shall describe why the Contractor agrees with the <<YOUR AGENCY>> assessment and provide specific reasons and references that support the Contractor's position. For each question in <<YOUR AGENCY>>'s completed questionnaire where the Contractor disagrees with the <<YOUR AGENCY>> assessment, the final report shall describe why the Contractor disagrees with the <<YOUR AGENCY>> assessment and provide specific reasons and references that support the Contractor's position. The final report shall be delivered in typed and electronic form. The Contractor shall be available to answer questions regarding their final report until the end to the period of performance. The electronic form of the final report can be delivered by e:mail or disk and shall be in Microsoft Word compatible format <<OR YOUR AGENCY STANDARD>>.

7.0 **Key Person Clause**

The Contractor's Program Manager shall meet or exceed all requirements under **Suitability Clearances and Minimum Experience Requirements**. Any change or substitution of the Program Manager after the Contractor's bid has been submitted shall be approved by <<YOUR AGENCY>>'s Project Officer in writing. The Contractor shall certify that all Contractor support staff working on this contract meet or exceed all requirements under **Suitability Clearances and Minimum Experience Requirements**.

8.0 **Security and Confidentiality of Information**

The Contractor shall sign a nondisclosure statement such that all information provided by <<YOUR AGENCY>> or obtained for use under this contract shall be considered sensitive and confidential and shall be maintained in a secure environment such that only authorized Contractor persons and <<YOUR AGENCY>> persons shall have access to it and shall not be disclosed to any unauthorized person without the Project Officer's written permission. <<YOUR AGENCY>> will arrange for the required level <<YOUR AGENCY STANDARD>> Contractor suitability clearances.

9.0 **Period of Performance**

The period of performance for completion shall be from the date of the award of this contract until <<INSERT>>.

10.0 **Schedule of Tasks/Deliverables**

Schedule of Deliverables

Unless otherwise stated in the Statement of Work, 1 (one) paper copy and 1 (one) electronic copy of each deliverable are to be delivered to the Project Officer.

<u>Task</u>	<u>Deliverable</u>	<u>Due Date</u>
--------------------	---------------------------	------------------------

within # of calendar days after award)

1	Complete and Deliver finger print and suitability clearance and building access forms	3 Days
2	Post Award Meeting	5 Days
<u>(The following Due Dates are within # of calendar days after award or within number of calendar days of <<YOUR AGENCY’S>> delivery to the contractor of the completed questionnaire, whichever is later)</u>		
3	Research and Review Documents	35 Days
4	Prepare and Deliver Draft Report	35 Days
(7 Days—Internal <<YOUR AGENCY>> Review)		
5	Meet with <<YOUR AGENCY>> Personnel	42 Days
6	Prepare and Deliver Meeting Minutes	45 Days
7	Prepare and Deliver Final Report	49 Days

11.0 **Proposal Instructions**

The proposal shall demonstrate the offeror’s understanding of the requirements. This shall include, but not be limited to, all relevant personnel and corporate experience and credentials. The government discourages excessive elaboration. Nevertheless, the Offerors should recognize that the Government’s evaluation will consider the merits of the Offeror’s technical approach and capabilities, experience, project management and past performance in response to the specific requirements of this procurement. It is not sufficient to merely reiterate the requirements in the statement of work; the work to be performed, and the work cited as examples of past performance, must be described in sufficient detail to allow the reviewer(s) to evaluate the merits of the offeror’s proposal and past performance information.

The Technical Proposal shall include the following four parts:

1. Experience of Proposed Program Manager and Support Staff

This section shall discuss the experience and relevancy of the staff proposed for this contract. The Program Manager’s resume shall document their experience, addressing all areas covered in the Statement of Work (SOW), particularly the minimum requirements as described in Parts 4.0 and 12.0 of the SOW. The resume of the key personnel (program manager and support staff) proposed shall be incorporated into an appendix.

The Offeror shall provide a statement certifying that all Contractor support staff (including subcontractors, if any) that work on this contract meet or exceed all experience requirements as described in Parts 4.0 and 12.0 of the SOW. The certifying statement shall be signed by a responsible representative of the offeror (include their title) and incorporated into an appendix.

2. Technical Approach

This section shall provide a comprehensive statement of the contractor's proposed technical approach to the requirement, addressing all areas covered in the SOW, particularly the detailed description of tasks, activities and deliverables provided in Part 6.0 of the SOW. It should include a detailed description of the proposed research methodology based on the parameters furnished.

3. Contractor Experience and Past Performance

This section shall discuss the offeror's experience and past performance in conducting projects of a type similar in scope, size, and complexity to that described in the SOW. Experience information includes relevant contracts, including sample instruments, for the same or similar types of items/services. The Offeror shall include at least three citations/references that adequately demonstrate its experience and record of past performance. Citations/references must be currently active, or must have been completed within the last three years. The offeror must submit the following information for all citations/references:

- A. Client's Name, Address.
- B. Name of the Contracting Officer (CO), the Contracting Officer's Technical Representative (COTR), Point-of-Contact (POC) and Telephone Number of both (including area code and extension, if appropriate). For contracts performed for non-government customers, one POC may be given. This POC should be the equivalent of a Government COTR or CO.
- C. Brief description of the services rendered.
- D. Show the type of contract, dollar value of the contract at time of award, cumulative dollar value of contract to date, and period of performance. Indicate whether or not contract renewal options were exercised.
- E. Indicate the percentage of staff turnover per contract year.
- F. Describe any significant problems that arose and explain how they were resolved.

4. Project Management Plan

This section of the proposal shall provide a description of the Offeror's overall project management in response to the specific needs of the current requirement as well as information organized around the tasks described in the SOW. The offeror shall provide a chart of proposed staff hours according to the tasks, activities and deliverables specified in the proposal (without prices). The Offeror shall indicate the percentage of the tasks, if any, that will be accomplished by subcontracting and the specific tasks that will be accomplished by subcontractors.

12.0 **Evaluation Information**

A. Technical Evaluation Criteria

The technical review will include the following factors listed in descending order of importance:

I. **Contractor Program Manager's and Support Staff's Past Experience**

This factor will be evaluated on the basis of the offeror's Project Manager's experience in conducting projects of a type similar to that described in the statement of work. The proposed Project Manager must meet the following minimum requirements:

Program Manager: Demonstrated, in-depth knowledge consistent with security principles and best practices as reflected in the CIO Council's *Federal Information Technology Security Assessment Framework, Government Information Security Reform Act, Computer Security Act*, Office of Management and Budget A-130 and NIST 800-18.

Ten years experience in consulting or conducting information systems security analyses or reviews.

Demonstrated experience in assessing large civilian or non-civilian government Security Programs.

Demonstrated experience in writing and presenting reports to Executive level personnel.

A college degree in Computer Science or Information Management

or

Currently a Certified Information Systems Security Professional (CISSP)

or

Documented experience in all 10 Common Body of Knowledge areas:

- Access Control Systems and Methodology,

- Telecommunications and Network Security,
- Security Management Practices,
- Application and Systems Development Security,
- Cryptography,
- Security Architecture and Models,
- Computer Operations Security,
- Business Continuity Planning and Disaster Recovery Planning,
- Law, Investigation, and Ethics, and
- Physical Security.

This factor will also be evaluated on the basis of the proposed support staff's experience. Proposed support staff must have three years experience which demonstrates knowledge in the area of Computer Information Systems Security.

II. Technical Approach

The offeror will be evaluated on their proposed technical approach for accomplishing the work to be performed under this task order, including all areas described in the Statement of Work (SOW). The offeror's understanding of the contract requirements and ability to demonstrate that the offeror has a plan for completing these requirements in a timely and high quality manner will be measured.

III. Contractor Experience

This factor will be evaluated on the basis of the offeror's experience in conducting projects of a type similar in size, scope, and complexity to that described in the statement of work. This assessment will be made by reviewing the information submitted by the offeror, including sample instruments, any information received when contacting references, and information available from other public and private sources.

IV. Past Performance

This technical evaluation area will consider the offeror's past performance in managing and conducting projects of similar size, scope, and complexity to that of this solicitation. Evaluation of this criteria will be made by reviewing the information submitted by the offeror, any information received when contacting references, and information available from other public and private sources. Evaluation of this criterion will be based on the extent to which the corporate experience reflects customer satisfaction in the areas of: timeliness of deliverables; competency; accuracy of work products; responsiveness to customer requirements; initiative and innovation; staffing (i.e., assigning/hiring/training qualified personnel and, when necessary, providing timely replacements); and subcontractors—effective and efficient management of subcontractors, if any, and utilization of quality subcontractors.

In evaluating past performance, the Government reserves the right to contact references as deemed necessary to enable adequate evaluation of proposals. The Government is not limited to the references listed by the offeror—the Government reserves the right to contact any relevant references for past performance information using public and private sources. The Government is not required to make more than 2 attempts to contact any given reference.

V. Project Management Plan

This factor will be evaluated on the basis of the offeror's overall project management plan, including proposed staff hours according to the tasks, activities and deliverables specified in the proposal (without prices), and in response to the specific needs of the current requirement as well as information organized around the tasks described in the SOW. The Offeror shall indicate the percentage of the tasks, if any, that will be accomplished by subcontracting and the specific tasks that will be accomplished by subcontractors. This assessment will be made by reviewing the information submitted by the offeror.

B. Basis for Award

Award will be made to the offeror whose offer represents the best value for the government, price and other factors considered. For this award, technical quality (including the experience of the project manager, corporate experience, past performance, and technical approach) is significantly more important than price.